WINTER 23/24

CyberEd MAGAZINE

Top Ten Cybersecurity Threats in 2024

PAGE 8

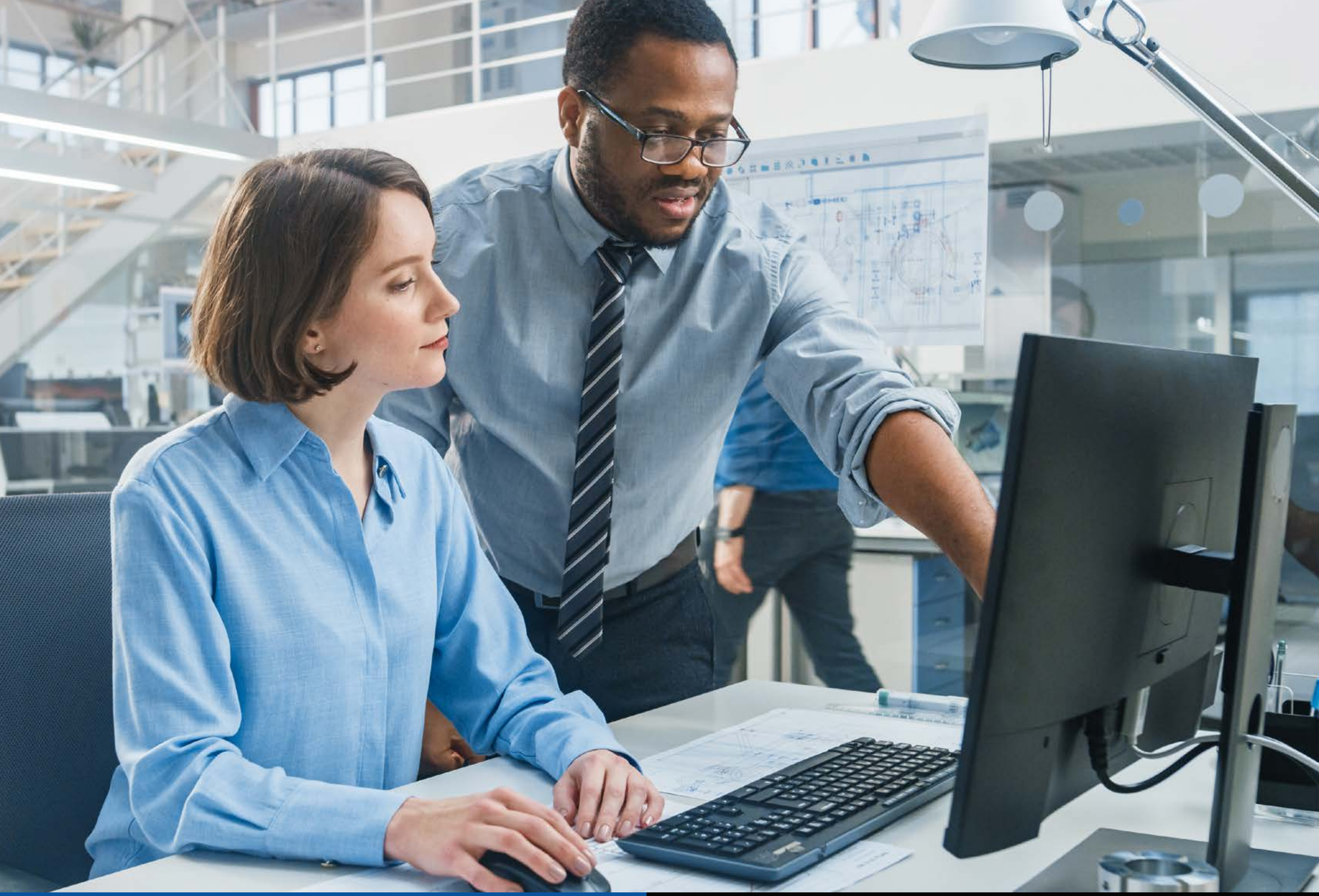
COVER STORY INTERVIEW

Fostering a Strong Cybersecurity Culture in 2024

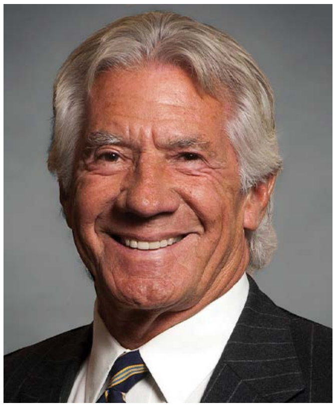
A Conversation with Steve King

PAGE 12

Steve King
Senior Vice President,
CyberEd.io



Letter from the Senior Vice President



Steve King
Senior Vice President,
CyberEd.io

King is a seasoned technology executive with more than 25 years of experience in the cybersecurity industry. He is currently Senior Vice President for CyberEd.io, the cybersecurity education division of ISMG. He began his career as the West Coast managing partner of MarchFIRST, Inc. overseeing significant client projects, and later founded Endymion Systems, which was eventually acquired by IBM. Throughout his career, Steve has held leadership positions in startups, such as VIP/SeeCommerce and Netswitch Technology Management, contributing to their growth and success.

Welcome to the Winter 23/24 issue of CyberEd Magazine!

CyberEd Magazine is back with a new quarterly edition, coinciding with the relaunch of CyberEd.io, the cybersecurity education division of Information Security Media Group. Our winter 23/24 issue brings valuable insights into cybersecurity education, along with a glimpse of our plans for the year ahead. We've gathered wisdom from an array of cybersecurity thought leaders to help keep you updated, and hopefully, entertained too.

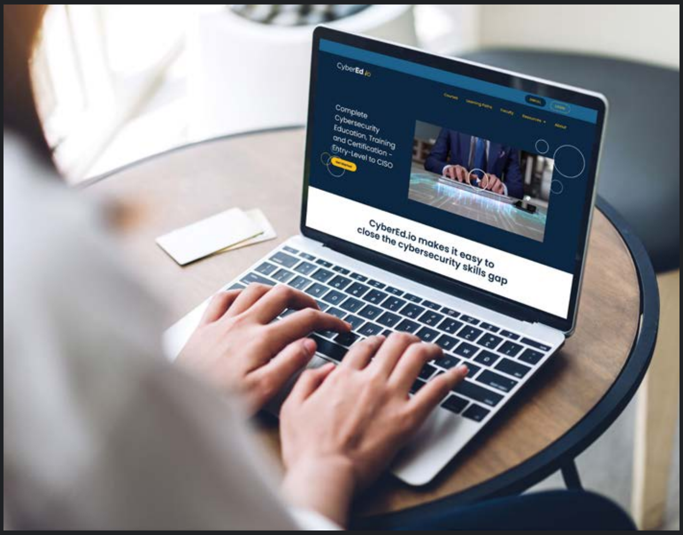
This issue includes my first interview conducted by our CyberEd team. We all wanted to kick off the new year with a bang, and this interview enables me to underscore the need to strengthen our cybersecurity culture and discuss how a lack of flexibility and innovation are likely to block organizations from keeping up with the pace of AI changes expected in the year ahead. You'll also find my top ten cybersecurity threat predictions for 2024. And key takeaways from recent cybersecurity conferences, along with a closer look at CyberEd Learning Paths for Security Engineering and Forensics are also described in this issue. In addition, recent podcasts highlighted in this issue include one featuring Amit Yoran, Chairman and CEO at Tenable, on the critical need for increased CISA funding. A separate podcast featuring Jenny Hedderman Esq., Risk Counsel in the Statewide Risk Management Team for the Massachusetts Office of the Comptroller, goes over the Joe Sullivan case, generative AI regulations, and best practices in cybersecurity governance.

We are working hard to usher in a new era of cybersecurity awareness and hope you'll enjoy the valuable insights and resources we've shared for your use.

Warm regards,

Steve King
Senior Vice President, CyberEd.io
Information Security Media Group

NEW COURSES


CyberEd.io
Complete Cybersecurity Education, Training and Certification - Entry-Level to CISO
CyberEd.io makes it easy to close the cybersecurity skills gap

We're constantly updating the CyberEd.io platform with new course content including lectures from the world's leading cybersecurity and technology experts.

Issues, Topics and Interviews

SPRING

COVER STORY:
Interview with John Kindervag

LEARNING PATH SPOTLIGHT:
Cloud Security & Risk Analysis

SUMMER

COVER STORY:
Interview with Chase Cunningham

LEARNING PATH SPOTLIGHT:
Security Warrior & Penetration Testing

FALL

COVER STORY:
Interview with Richard Bird

LEARNING PATH SPOTLIGHT:
Digital Forensics & ICS

WINTER

COVER STORY:
Interview Steve King

LEARNING PATH SPOTLIGHT:
Security Engineering & SOC

CyberEd MAGAZINE

CyberEd Magazine Editorial
Chief Executive Officer **SANJAY KALRA**
General Manager **MICHAEL D'AGOSTINO**
Senior Vice President **STEVE KING**
Dir. of Content Dev. and Managed Services **KYLE SCHMECHEL**
Executive Editor **BARBARA REIMERS**
Director of Global Creative Strategy **ALEXANDRA PEREZ**
Lead Graphic Designer **CAITLIN PERSICHILLI**
Social Media Coordinator **PURTIKA PANDEY**

ISMG Editorial
Senior Vice President Editorial **TOM FIELD**
Executive Editor **MARIANNE K. MCGEE**
Executive Editor **MATHEW J. SCHWARTZ**
Managing Editor **GEETHA NANDIKOTKUR**
Managing Editor **TONY MORBIN**
Managing Director **VARUN HARAN**
Director Global News Desk **BRIAN PERIERA**
Editorial Director, News **DAVID PERERA**
Editorial Director **CAL HARRISON**
Principal Correspondent **SUPARNA GOSWAMI**
Director of Production **ANNA DELANEY**

Contact
902 Carnegie Center
Princeton, NJ 08540

Toll Free: (800) 944-0401
ismg.io

iSMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Our 34 global media properties provide security professionals and senior decision makers with industry- and geo-specific news, research and educational events.

www.ismg.io

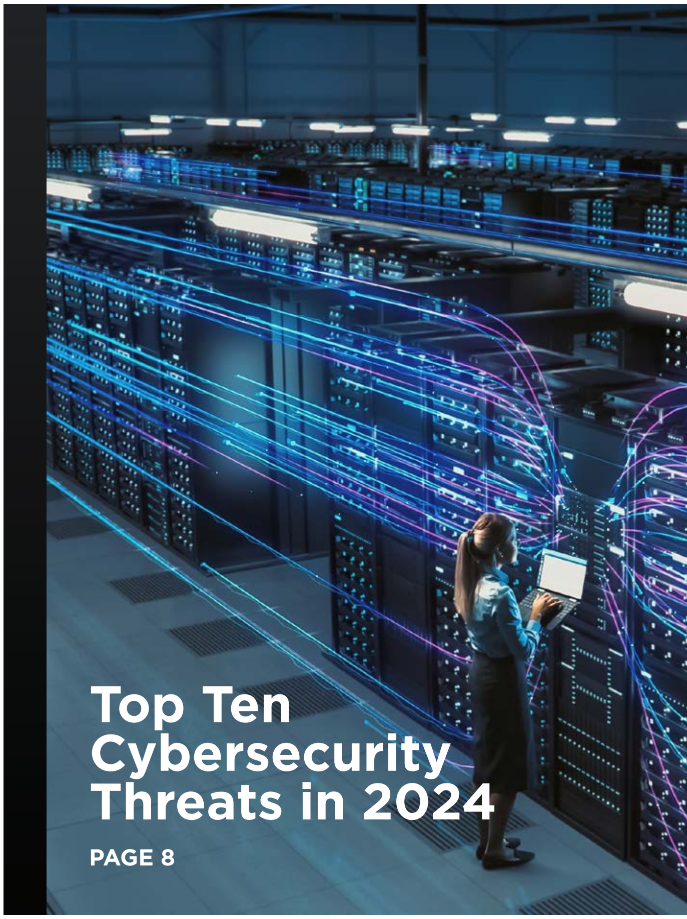
Table of Contents

COVER STORY INTERVIEW

Fostering a Strong Cybersecurity Culture in 2024

A Conversation with Steve King

PAGE 12



Top Ten Cybersecurity Threats in 2024

PAGE 8

A Roundup of Recent Cybersecurity Events

Takeaways from key cybersecurity conferences

MUMBAI CYBERSECURITY SUMMIT 2023

Last November, ISMG's Mumbai Cybersecurity Summit focused on digital resilience, security, growth and business transformation, and included security leaders from banking and financial services, computer software, healthcare, insurance, government and education.

Source: Mumbai Cybersecurity Summit 2023

Sameer Ratolikar, senior executive, VP and CISO at HDFC Bank Ltd., expounded on the role of CISOs as leaders and role models, highlighting the need for strategic thinking, leadership to counter information warfare, organizational resilience, and the integration of security into each organization's DNA.

In a keynote address about Digital India, Dr. Yoginder Talwar, Sr. GM/HoD-Tender and CISO at National Informatics Centre Services Inc., described how the Digital India movement, propelled by the Digital India Act, has been a catalyst for economic growth. He focused on the Act's transformative impact on CISOs and outlined strategies to safeguard digital innovations, including the use of artificial intelligence and machine learning to fortify security defenses.

The summit culminated in a panel discussion on the "Top Technologies That Will Shape Your Enterprise in 2024." Government and industry security leaders touched on the significance of India's Digital Personal Data Protection Act of 2023, emphasizing the need to invest in defenses to counter evolving attack tactics. Summit sessions underscored how AI-powered solutions can facilitate threat detection, incident response and robust defense mechanisms, to help prepare CISOs for challenges emerging today and in the future.

Source: Black Hat Europe 2023

BLACK HAT EUROPE 2023

Last December's Black Hat Europe highlighted key topics involving cloud security, network security, AI/ML, cyber-physical systems and IoT.

In a keynote address, Ollie Whitehouse, CTO for the National Cyber Security Center advocated the idea of catching adversaries off guard with unexpected strategies, drawing parallels with Google's DeepMind AI program, which defeated human players in Go by employing unprecedented moves.

In another keynote, Joe Sullivan, former CSO at Facebook, Uber and Cloudflare, shared insights from the U.S. government's case against him, in which he was charged and convicted of a felony following a 2016 data breach during his tenure at Uber. Sullivan used his case to demonstrate the shifting professional challenges facing CISOs. He underscored how CISOs must maintain technical expertise while evolving into effective senior executives capable of strategic leadership. He challenged the audience to plan for their professional trajectories, asking them whether they preferred to remain deeply immersed in technical intricacies, or ascend to senior leadership roles.

Jeff Moss, the founder of Black Hat, delved into cybersecurity challenges anticipated in the years ahead including a surge in misinformation campaigns during global elections, as well as China's readiness to conquer Taiwan. He urged organizations to review their cybersecurity posture and incident response plans in anticipation of potential mass disruptions.

The overarching messages from both global events underscored how cybersecurity professionals must embrace change, evolve and cultivate strategic leadership capabilities.

Top Ten Cybersecurity Threats in 2024

By Steve King

In 2024, I expect the cybersecurity landscape to evolve with new threats emerging alongside advances in artificial intelligence (AI) and Quantum technology. Here are my top 10 predictions for cybersecurity threats in 2024:

1 ADVANCED RANSOMWARE TACTICS

Ransomware attacks are likely to become more sophisticated. Cybercriminals will easily leverage AI to enhance their targeting capabilities, making ransomware more personalized and harder to detect. Deep fakes, and ultra-convincing emails and telephone calls will evade detection and drive human behaviors to cooperate with privileged asset corruption and careless responses to threat vectors, regardless of any staffer's prior training. We will also see an increase in 'Ransomware-as-a-Service' models, enabling even less skilled attackers to launch devastating ransomware campaigns.

2 AI-DRIVEN CYBER ATTACKS

AI is a double-edged sword in cybersecurity. While it can improve security measures, it also provides cybercriminals with powerful tools. AI can be used to automate attacks, create more convincing phishing campaigns, and produce deepfakes for social engineering, so our best response is to embrace a form of Human Risk Management where we monitor all employee behavior and interaction with security products throughout the enterprise and create risk scores for each element. Employees with the most dangerous risk scores can be identified for specific training designed to mitigate specific risks. Those risk scores can be monitored to assure that progress is made over time, or if additional intercession is required. This trend represents a significant escalation in the complexity and potential impact of cyberattacks.

3 REMOTE WORK INFRASTRUCTURE EXPLOITS

With the continuing trend of remote work, even in moderate forms, the attack surface remains expanded. Hackers are expected to increasingly target remote work infrastructures, exploiting vulnerabilities in VPNs, cloud services, and remote desktop protocols. These attacks will lead to unauthorized access to sensitive corporate networks and data. The answer is still to eliminate the use of VPNs and patch vulnerable Microsoft products that enable remote code execution (RCE) and use human risk management monitoring to gain visibility into potential future risks through behavior analysis

4

SUPPLY CHAIN CYBER ATTACKS

I expect supply chain attacks, where hackers target less secure elements in the supply chain to attack more secure targets, to continue rising. As the bad guys get better at compromising trusted third-party software and hardware, they will find new gateways to multiple victims at once. A serious part of hygiene must include third party provider audits of their cybersecurity readiness, resilience and overall risk posture. Hard decisions must be made. Trust no one's assessment but your own.

5

CRITICAL INFRASTRUCTURE TARGETING

Cyberattacks on critical national infrastructures, such as energy grids, healthcare systems, wastewater treatment facilities and transportation networks, will increase. These attacks will be motivated by geopolitical conflicts and financial gain, but the potential to cause widespread disruption and harm is far greater in this attack class than most others. Colonial Pipeline is a living example of what happens when a gas pipeline is taken down. Societal unrest in an election season is a classic example of cybersecurity psyops designed to divide a nation based on cognitive and information warfare and propaganda. We will see much more of this next year.

6

IOT DEVICE VULNERABILITIES

As the number of connected IoT devices grows, so does their attractiveness as cyberattack targets. And since we are the world's moist connected nation, the U.S. is at the greatest risk and is most vulnerable to cyberattacks. Many such devices have inadequate security features, making them easy targets for hackers to create large-scale botnets or gain access to networks. Our challenge is to scale our remedies. However, we are talking about 300-400 million users resistant to change and/or any interventionist style of hygiene, or required training, or even upgraded password policies.

7

MOBILE DEVICE EXPLOITS

With increasing reliance on mobile devices, attacks on these platforms are expected to substantially rise. This includes exploiting vulnerabilities in mobile operating systems, apps, and mobile-centric technologies, like 5G. We know TikTok is an active threat, yet we don't cancel the app. We still use millions of Chinese Huawei parts in our telecom systems, which are capable of and do consume IP and critical design knowledge about our communication systems. Yet somehow, we seem incapable of implementing an outright ban.

8

DATA PRIVACY BREACHES

Personal data privacy breaches will also continue to rise. Companies will face sophisticated attacks aimed at stealing sensitive personal information, which will be used for identity theft, financial fraud, or sold on the dark web in the form of complete dossiers for criminals to establish full identities and go after complete individual lifestyles without detection.

9

STATE-SPONSORED CYBER WARFARE

Cyber warfare activities sponsored by nation-states will increase. These activities include espionage, sabotage, and influence campaigns. The blurred lines between state actors and cybercriminals will lead to complex conflicts with global implications. Combined with psyops campaigns designed to create hatred among tribes, the effect of these two elements combined together will be powerful. Hamas v. Israel is a classic case in point.

10 QUANTUM COMPUTING AND CRYPTOGRAPHY

As quantum computing advances, it poses a threat to current cryptographic standards. Quantum computers have the potential to break many of the cryptographic algorithms currently in use, leading to a potential 'crypto apocalypse'. Organizations must start preparing for post-quantum cryptography to secure communications against this emerging threat. I only know of a few banks so far that are doing so.

FINAL REFLECTIONS

The cybersecurity landscape in 2024 is poised to be dynamic and challenging, with a blend of technological advancements and sophisticated attack methodologies, along with an apparent 'lack of will' to do anything to prevent or protect serious incidents.

Organizations must strive to be vigilant, continually update their security strategies, and invest in workforce training and the current security solutions that will help them mitigate the emerging risks, most of which are hygienic in nature.

API security, which is included in the first two predictions, is a reminder that a category of threat is not the same as a threat vector. Malware must be included in every breach by definition, and is the single most dangerous threat, but it is a weapon rather than a vector. API vulnerabilities are like phishing attacks. Nothing happens until either is exploited.

2024 could be the worst year in the history of our art, despite the fact that cybersecurity has become a critical component of organizational strategy and national security. AI has emerged as the transformational, yet invisible enabler.

Happy new year and best of luck.

Fostering a Strong Cybersecurity Culture in 2024

A Conversation with Steve King

Steve King is a seasoned technology executive with more than 25 years of experience in the cybersecurity industry. He is currently Senior Vice President for CyberEd.io, the cybersecurity education division of ISMG. He began his career as the West Coast managing partner of MarchFIRST, Inc. overseeing significant client projects, and later founded Endymion Systems, which was eventually acquired by IBM. Throughout his career, Steve has held leadership positions in startups, such as VIP/SeeCommerce and Netswitch Technology Management, contributing to their growth and success. Currently, he's actively involved in the cybersecurity community, serving on multiple advisory boards and holding engineering patents, while maintaining certifications in CISM (Certified Information Security Management) and as a CISSP (Certified Information Systems Security Professional). Steve's strong educational background includes studies at U.C. Berkeley and at both Stanford and Lincoln University law schools, further solidifying his expertise in the field.

In a recent interview with CyberEd.io, Steve King talks about the future of AI and key cybersecurity threats and trends to watch in 2024. He anticipates core business disruption for organizations that are late or lagging in their adoption of AI.

From a cybersecurity perspective, how should we characterize the year 2023?

In a word, it's been dismal. We saw more breaches. And cyberattacks are getting more sophisticated. Take for example the recent breach reported by Proofpoint. Threat actors targeted recruiters by sending them a direct email. The attacker pretends to be an individual interested in a job

The email does not include any malicious content. Once the recruiter replies to the email, the attacker replies with a link leading to an attacker-controlled website posing as an individual's resumé.

An alternative method used by the threat actor consists of replying to the recruiter with a PDF or Microsoft Office Word file containing instructions to visit the fake resume website.

The website employs filtering mechanisms to assess whether a subsequent phase of the attack should be initiated. If the criteria for filtering are not met, the user is presented with a plain text resume. If the filtering checks are successfully passed, the user is redirected to the candidate website, where they are prompted to solve a CAPTCHA.

Upon successful completion, the user is provided with a ZIP file that includes a Microsoft Windows shortcut (LNK) file. A LNK file is a Windows shortcut that serves as a pointer to open a file, folder, or application. If executed, the LNK file abuses legitimate software ie4uinit.exe to download and run a script from a location stored in the ie4uinit.inf file. This technique is known as 'Living off the Land' and consists of using existing legitimate software and tools to accomplish malicious actions on the system and minimizing the likelihood of being detected.

The downloaded script decrypts and drops a dynamic link library (DLL), which is a collection of small programs that larger programs can load when needed to complete specific tasks. Then it attempts to create a new process to execute the DLL by using Windows Management Instrumentation (WMI). If this attempt fails, the script tries another approach by using the ActiveX Object Run method.

Once the DLL is executed, it decrypts malware along with the legitimate Microsoft command line transformation utility, MSXSL.ex. Then, it initiates the creation of the MSXSL process using the WMI service. The DLL deletes itself once the infecting process is completed.

According to Proofpoint, the malware enables persistence and profiling of the infected system, and it's also often used to download additional payloads.

Bottom line: THAT is a sophisticated attack. And we continue to demonstrate over and over that we don't have the skill or software to detect this type of attack while it's happening. Now, the situation is only going to get worse because the bad guys are using generative AI (GAI).

What do you see as the most significant cybersecurity threats or trends to watch in 2024?

An increasing reluctance to underwrite cyber-insurance policies will lead to skinny coverage with payout caps and multiple exceptions, along with much more rigorous qualifying requirements now that insurers have a better sense of how to assess risks, and what to look for.

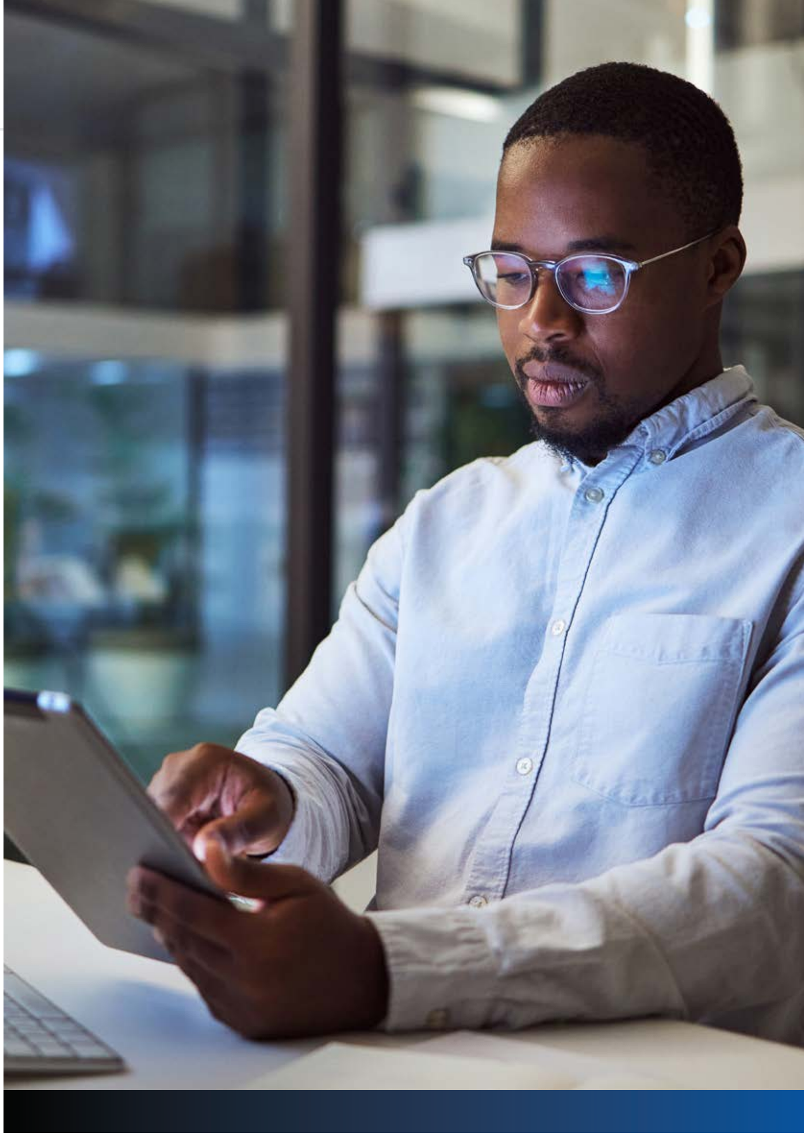
Continuing complexity as more tools are layered into networks in attempts to solve point problems and less visibility and fractured observability as a result. Net outcome is weaker defenses.

Leveraged **generative AI (GAI) will create far more sophisticated attack vectors**

and vastly improved phishing and social engineering campaigns. The percentage of people fooled by these attacks will also dramatically increase.

Critical infrastructure risks will increase as we continue to underestimate the threat from global threat actors, while dismissing the need for corrective action. For example, the recent cyberattack involving Unitronics Programmable Logic Controllers (PLCs), is significant. This attack implicated the Iranian Islamic Revolutionary Guard Corps (IGRC) in a supply chain attack that impacted multiple critical infrastructures in the United States and affected international users. This attack targeted Israeli-made Unitronics PLCs, exploiting vulnerabilities through their customer networks. So far, the response from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has been criticized as inadequate. CISA primarily addressed IT issues without delving into the specific risks posed to industrial PLCs. This oversight is dangerous because the superficial defacements seen in the attack may mask deeper, more harmful manipulations of PLC logic.

This incident bears a resemblance to the Stuxnet attack, which was focused on the PLCs of centrifuges in Iran, leading to speculation about whether this could be a form of retribution. However, the attack pattern observed with Unitronics PLCs is not exclusive to the Unitronics brand, or to the water and wastewater sectors. Instead, **this incident underscores a broader security concern: the prevalence of default passwords, a known security vulnerability in IT, operational technology (OT), and control systems across various vendors.**



Given the widespread use of Unitronics PLCs in the U.S., and around the world, the responses and alerts issued by CISA, and Common Vulnerabilities and Exposures (CVE) related to these PLCs have been deemed inadequate. This stance leaves U.S. critical infrastructures more vulnerable to similar attacks in the future. The root of this vulnerability involves a lack of visibility into the access points to OT networks, and a resulting lack of knowledge about who resides therein, what exactly they are watching, and which actions trigger a C&C attack command. [C&C is a method cybercriminals use to communicate with compromised devices on a target organization's network. In a C&C attack, an attacker uses a server to send commands to, and receive data from, computers compromised by malware.]

What best practices would you recommend to foster a strong cybersecurity culture and reduce the risk of insider threats in 2024?

Education, education and education. Every enterprise needs to get smarter about threats, along with the best practices required to protect against cyberattacks. Meanwhile, security teams must invest time and energy into advanced training, especially on offensive specialties. CISOs need to keep current with all of the rapid advances in technology, processes and compliance issues, while the non-technical C-suite needs to expand their understanding of cybersecurity, far more than they do today.

One advance likely to make an enormous difference is CyberEd.io's approach to Human Risk Management (HRM), a new category recognized by both Gartner and Forrester that focuses on employee behaviors, and guides training to employees who need it most and carry the highest risk scores. Instead of old-school Security Awareness Training for everyone – which no one likes and is typically conducted twice a year – HRM training is based on continuous monitoring of all employees and their behaviors around and with existing security products.

When a risk score exceeds a specific pre-determined threshold, alerts are sent to the security team and the monitored employee receives polite nudges reminding them of proper security behavior. The security team may also arrange appropriate corrective training from our large library of coursework to help each employee understand and overcome any negative habits and apply best practices that will lower their risk score, along with the risk score for the enterprise as well.

Best of all, our new HRM training category costs less than the combination of traditional Security Awareness Training, combined with conventional cybersecurity coursework from current training market participants

In 2023, AI achieved broad adoption. In 2024, the potential for transformation appears limitless. Any thoughts on the future of AI?

Ultimately, if a business hasn't developed an AI strategy, it's likely already too late. You will lose market share and core business disruption will occur for those who are in the late majority, along with those in the late adoption and laggard categories. **A lack of flexibility and innovation are likely to block organizations from being able to keep up with the pace of change.** Meanwhile, new AI business entrants won't have much to lose

in terms of risk and are likely to embrace generative AI to move better and faster.

On the other hand, AI also represents an enormous set of threats that emanate from poisoned data in large language models (LLMs). The most likely threats today emerge from: a lack of training; a lack of adequate security policies; a lack of guardrails and/or monitoring of network use; leaky abstractions; privacy violations; and malicious scaling; to name a few.

By this time next year, we will be amazed as we assess the impact of AI on business operations, and on the world around us. Unfortunately, **I'm confident we will see a 75% loss of jobs within 12 months.**

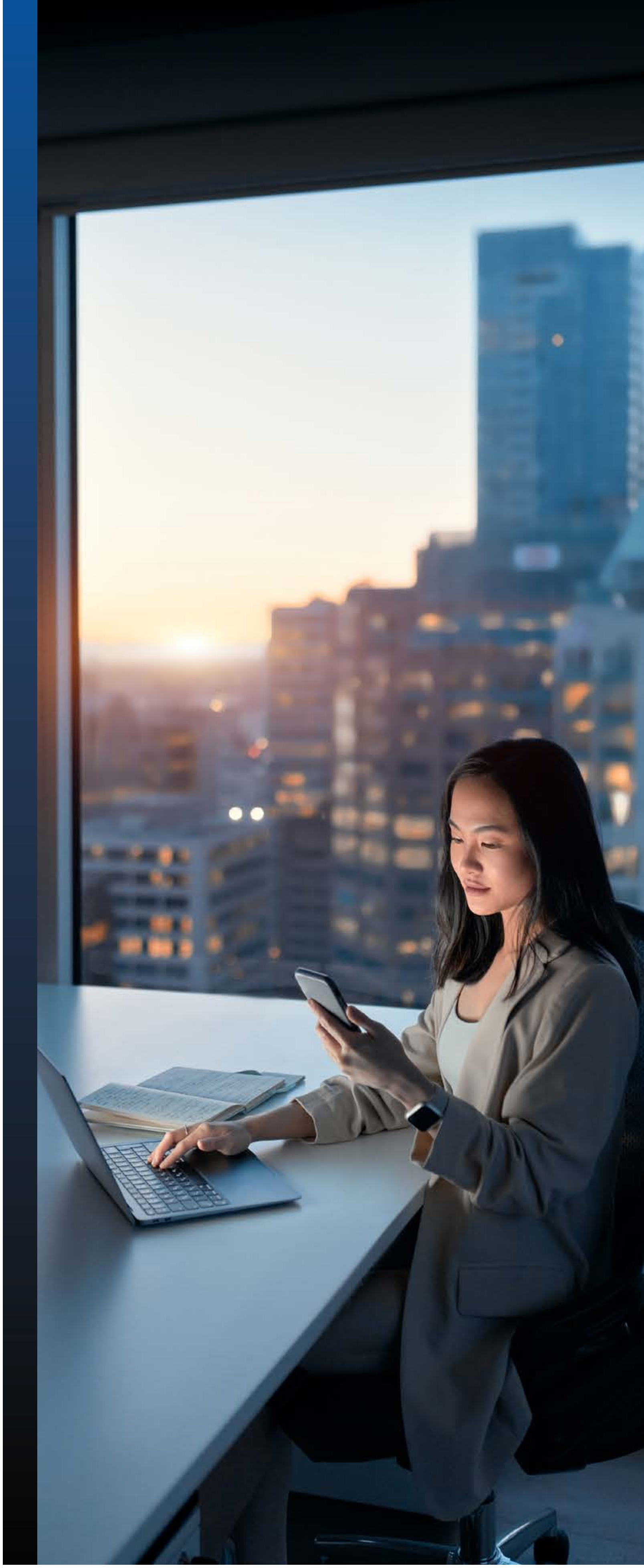
What was the most valuable lesson you learned as a CISO? And how have you applied what you learned to the evolving cybersecurity realm in 2024?

Ha! My biggest lesson was to never do that again! To be fair, when I held the CISO role for a large financial institution, the world was pretty different than it is today. Threats were better understood, less clever and less vile. We also did a better job of hygiene than we do today. Our networks were far less complex. The technology moved more slowly. AI only appeared in threat detection schemes in the form of discriminative AI used in algorithms to detect anomalistic behavior. We had no cloud native apps and complex containerization was only an emerging threat on the horizon. At the same time, the CEO and board of directors (BoDs) were responsible for the corporation's state of health relative to enterprise risk – not the CISO. The enterprise risk management (ERM) folks reported directly to the board, the CFO or the CEO, but not to the CISO. In fact, a CISO was not yet a C-level officer and did not hold fiduciary care duty or responsibility. S/he also was never protected by Directors and Officers (D&O) insurance coverage.

Now, we have seen the prosecution of CISOs for breaches, while the rest of the C-suite was protected by non-prosecution agreements in return for their testimony against the CISO. Depending on the depth, breadth and enthusiasm of regulatory oversight agencies, prosecutors and juries, events such as the Uber breach and the SolarWinds breach are likely to result in felony verdicts and potential prison sentences.

I believe this trend will increase, largely due to a combination of ill-informed CISO candidates, higher CISO compensation plans, trial results and the authority and self-preserving instincts of those in C-suites and on BoDs. I also think as a result, **we will see fewer candidates for CISO job roles**.

History is written by the victors, and this truism will not change for those working in cybersecurity.



Cultivating a Resilient Cybersecurity Program

Highlights from CyberEd's Latest Research Report

In the ever-changing digital landscape, organizations are confronted with an array of evolving cyberthreats that demand proactive and robust defensive strategies.

The usual "whack-a-mole" approach of addressing threats individually has proven ineffective, as it fails to provide the proactive, rapid responsiveness that is needed to improve resilience. Recognizing this, organizations are currently starting to shift to a more holistic approach to cybersecurity, one that acknowledges the interconnectedness of various security components and aims to comprehensively mitigate risks.

To navigate and defend the complex terrain of the internet operating environment, it is essential to harness a different mindset. A mindset serves as the lens through which individuals and organizations interpret and respond to situations, challenges, and opportunities. It encompasses attitudes, beliefs, thoughts, and perspectives that shape perception, behavior, and approach to developing an enterprise cybersecurity defense plan.

EMBRACING THE POWER OF MINDSETS

Key elements of a cybersecurity mindset include:

1. **Attitudes and Beliefs.** These are deeply held convictions about oneself, others, and the world influence how individuals perceive and interpret events, handle setbacks, and approach new situations. In the realm of cybersecurity, where chaos and uncertainty reign, these attitudes and beliefs play a significant role.
2. **Perception and Interpretation.** How individuals perceive and interpret information, experiences, and challenges determines whether they see obstacles as opportunities or setbacks. They may also view

failure as a learning experience, and approach change with curiosity and adaptability. Position awareness and situational awareness are greatly influenced by this mindset element.

3. **Thoughts and Self-Talk.** The thoughts and self-talk individuals engage in reflect their mindset. Positive mindsets involve constructive and empowering self-talk, while negative mindsets are characterized by self-doubt, criticism, and limiting beliefs.

4. **Growth Mindset vs. Fixed Mindset.** Mindsets can be categorized as either growth or fixed in nature. A growth mindset believes that abilities, intelligence, and skills can be developed and improved through deliberate effort, practice, and learning. In contrast, a fixed mindset assumes that abilities are fixed and unchangeable. A growth mindset is associated with resilience, a willingness to take on challenges, and a commitment to personal growth – all crucial aspects of executing a cyber defense program. To cultivate an organizational growth-oriented cybersecurity mindset, which is essential for executing an enterprise cyber defense plan, it's invaluable to grow three key mindsets: the Leadership Mindset, Warrior Mindset, and Zero-Trust Mindset.

COLLABORATIVE LEARNING AND HOLISTIC APPROACHES

Mental models act as a type of shorthand, helping us navigate our environment more efficiently. They are formed through a combination of personal beliefs, knowledge, experiences, and cultural influences. Collaborating with others and seeking diverse viewpoints allows individuals to broaden their mental models and gain a more comprehensive understanding of cybersecurity. By adopting a collaborative and holistic approach, organizations too can better address multiple dimensions of cybersecurity that ma otherwise be overlooked.

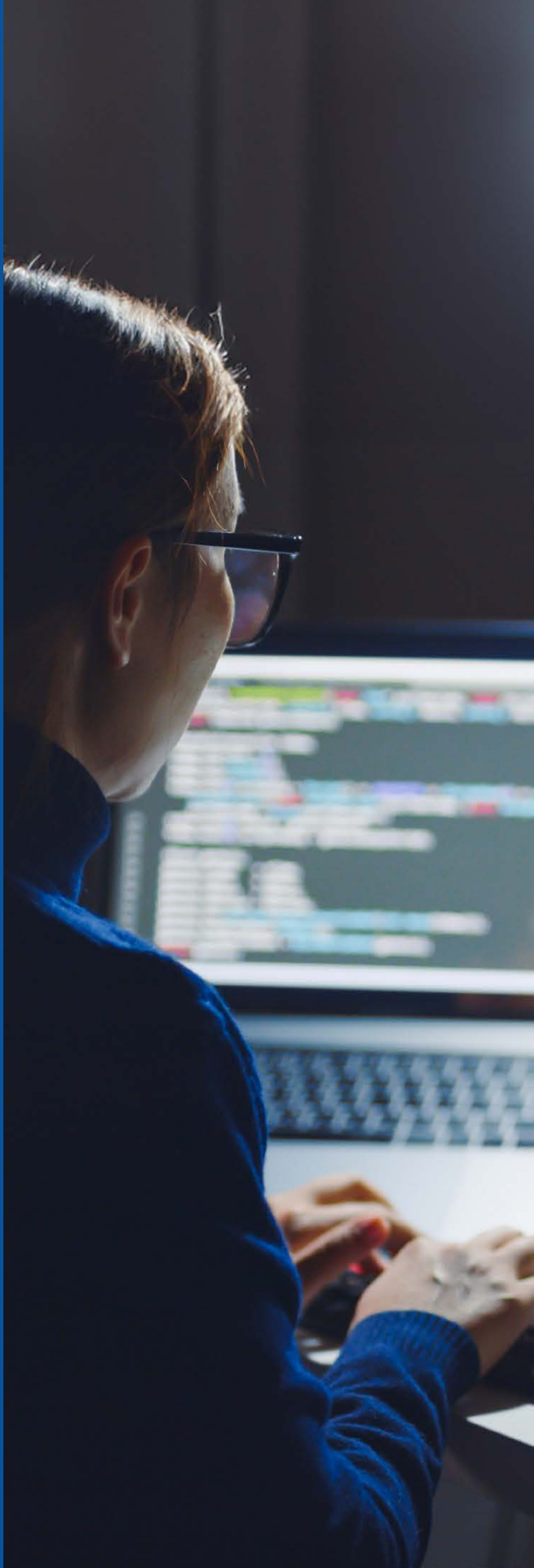
THE OODA LOOP AND DECISION-MAKING

The OODA (Observe, Orient, Decide, Act) Loop strategy model offers a valuable framework for collaborative decision-making. This model is specifically designed to develop holistic mental models that consider the broader context, interdependencies, and long-term consequences. The Orient phase, especially in the context of developing and implementing an enterprise cyber defense program, holds significant value as teams collaborate to build mental models for effective decision-making.

THE VALUE OF INTEGRATED MINDSETS

While each mindset brings unique perspectives, there are commonalities in their approaches. Proactive defense, risk assessment, and continuous improvement are key focal points across mindsets. By combining the visionary thinking and strategic planning of leaders, the courage and situational awareness of warriors, and the technical expertise and risk assessment capabilities of those with a zero trust mindset, organizations can develop a comprehensive and adaptable cyber defense program.

The full range of findings from this research report are available here.



CyberEd Featured Faculty

Chuck Brooks

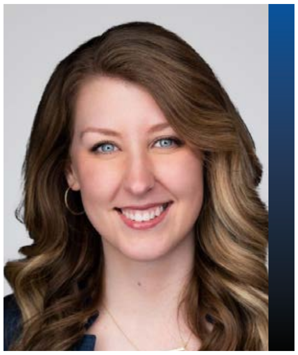
Adjunct Faculty, Georgetown University

Chuck Brooks is on the adjunct faculty in the Graduate Cybersecurity Program at Georgetown University. He is a featured writer/speaker/blogger on security, cybersecurity, CBRNE, artificial intelligence, IoT, science and technology, among other topics. He served as a cybersecurity SME for the U.S. Homeland Defense and Security Information Analysis Center. He's also a former technology partner advisor at the Bill and Melinda Gates Foundation, and he served on the EC-Council Global Advisory Board and the MIT Technology Review Advisory Board. Brooks has also served as VP for Homeland Security for Xerox, VP of Government Relations for SRA, and VP of R&D for Rapiscan. He is currently Chairman of the CompTIA New and Emerging Technologies committee.

Sam Curry

VP, CISO, Zscaler

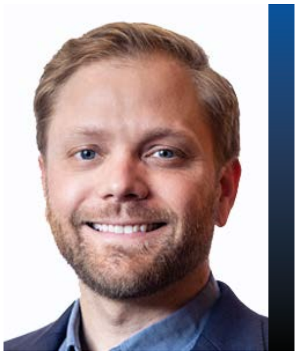
Sam Curry is a 30-year veteran who worked at Signal 9 Solutions, a start-up that invented the personal firewall, deployed the first commercial implementation of Blowfish, and devised early stealthy (symmetric key) VPN technology, which was later sold to McAfee. Curry went on to serve as Chief Security Architect and as head of Product for McAfee.com, before moving to leadership roles at RSA, including head of RSA labs at MIT and head of product, CTO, and Distinguished Engineer for EMC. After seven years with RSA, Curry served as SVP and CISO at MicroStrategy, then as CSO and CTO for Arbor Networks before it became Netscout, and later as CSO for Cybereason.



Kelly Hood

EVP and Cybersecurity Engineer, Optic Cyber Solutions

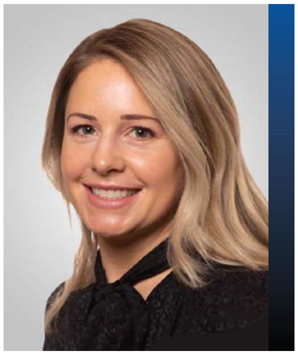
Kelly Hood is an EVP and cybersecurity engineering expert supporting organizations across sectors to develop and implement strategies to manage cybersecurity and privacy risks. She works with organizations to meet cybersecurity best practices, controls and standards, including the NIST Cybersecurity Framework, CMMC, SP 800-53, SP 800-171 and ISO 27001. She assisted the NIST Cybersecurity Framework team in the evolution and outreach of the Cybersecurity Framework.



Jimmy Mesta

Chief Technology Officer, KSOC

Jimmy Mesta is the founder and Chief Technology Officer at KSOC, the organization that triages risk across Kubernetes clusters in real time. He is responsible for the technological vision for the KSOC platform. Mesta, veteran security engineering leader focused on building cloud-native security solutions, Jimmy has held various leadership positions with enterprises navigating the growth of cloud services and containerization. At the Web App Firewall Innovator Signal Sciences (acquired by Fastly, Inc.), he led offensive and defensive teams across the Security and Engineering organizations while helping build modern, developer-friendly security solutions.



Lynn Peachey

Director of Business Development, Arete Incident Response

Lynn Peachey is an expert in the cyber insurance space. Currently, she serves as the director of business development, connecting clients and partners with cybersecurity solutions at Arete Incident Response, an insurance company and security insurance space. Previously earning her two bachelor's degrees from Rutgers University in New Jersey in psychology and industrial relations, then her JD from Pace University's Elizabeth Haub School of Law, Peachey is licensed in multiple states, including New York, California, Texas and Florida, as well as admitted to the New York and New Jersey Bar.

Nikki Robinson

STSM - Cyber Resiliency and Recovery, IBM

Dr. Nikki Robinson is a senior IBM Cybersecurity Engineer with 15+ years of experience in the IT and cybersecurity fields. Skilled in statistical data analysis, team leadership, penetration testing, and risk management, Nikki earned her doctorate in Cybersecurity from Capitol Technology University. Dr. Robinson is certified as a CISSP and CEH and is a member of the Board of Directors for InfraGard Maryland Chapter and provides support for InfraGard at the national level on the Journal Review Committee. Nikki teaches graduate-level courses in Quantitative Methods, Incident Response, and Healthcare Mobile Device Security at Touro College and Capitol Technology University.

Char Sample

Cybersecurity researcher, ICF

Dr. Char Sample is a cybersecurity researcher at ICF with decades of experience. Dr. Sample currently supports NSF research initiatives in Computer and Network Science research. Dr. Sample's current research focuses on deception, and the role of cultural values in cybersecurity events and decision-making. One other area of research that she finds interesting is the relationship between human cognition and machines. Currently, Dr. Sample is continuing research on modeling cyber behaviors by culture, data resilience, cyber-physical systems and industrial control systems and trustworthy artificial intelligence (TAI).

Greg Touhill

Director, CERT Division, Carnegie Mellon University
Software Engineering Institute

Gregory J. Touhill is director of the CERT Division of the Carnegie Mellon University (CMU) Software Engineering Institute (SEI), where he leads researchers who analyze security vulnerabilities, contribute to long-term improvements in cybersecurity, and develop cutting-edge training. Touhill once served as the first CISO of the U.S. government, and as deputy assistant secretary in the Department of Homeland Security's Office of Cybersecurity and Communications. Touhill is a 30-year U.S. Air Force combat veteran who retired with the rank of brigadier general. He holds degrees from Penn State University, the University of Southern California, and the Air War College. He maintains CISSP and CISM certifications and serves as an adjunct faculty member at CMU and Deakin University.

What's New in Security Awareness Training? *Everything!*

Spotlight on CyberEd Smart™ HRM

The market for traditional security awareness computer-based training (SACBT) has become standard, stable, and largely commoditized. There are literally over 50 different products on the market that purport to do some form of SACBT.

CISOs typically adopt these products for two primary purposes: phishing simulations and compliance. None of it works.

NO MOVEMENT FOR 10 YEARS

Not only does it not work today, but it also never did. In 2012, we could trace 95% of all cyber break-ins to a human error of one kind or another – a misconfiguration, an over-privileged user, an intentional multifactor authentication (MFA) workaround or an unintentional click on a malicious email offer. Today, after spending north of $60 Billion on SACBT, we can still trace 95% of cyber break-ins to human error.

Organizations that are serious about managing human risk are turning to new solutions, in a category known as Human Risk Management (HRM). Both Gartner and Forrester have acknowledged the category, named market leaders and created a Market Quadrant and Wave assessment for it.

Key elements include:

- **Behavioral Science** — Psychological principles that drive real behavior change
- **Data Integration** — Analyzing data from many sources for human behavior insights
- **Personalized Engagement** — Tailoring engagement to individual needs

TODAY'S NEW RULES

The objectives of human risk management are to achieve baseline compliance, target training to the employees most in need, and change culture to a model of security consciousness. That is to say, we no longer need to drag an entire company through dreaded SACBT training, which, by itself is a huge win.

The CyberEd.io Smart™ HRM solution uses our customers' installed security products to aggregate data about employee behaviors, and then parses that data in real-time with views by employee, department, team, function, etc. The views focus on a Risk Score, which is an immediate indicator of how risky or safe the behaviors are at each level. Risk scores that exceed a safe threshold are indicated for intercession at the individual or team level, using training from CyberEd's extensive library to address the specific risk.

Along with our continuous behavioral monitoring engine, we have visibility into the progress and/or regressions at each level so we can measure the efficacy of any training and identify gaps should any exist and do this step continuously, over time.

To learn more, contact us at cybered.io

The Future. Now.

CYBERSECURITY INSIGHTS PODCAST

A Letter to Congress about CISA Funding Cuts

Amit Yoran is the Chairman and Chief Executive Officer (CEO) at Tenable. He was also the Founding Director of the U.S. Computer Emergency Readiness Team (US-CERT) in the U.S. Department of Homeland Security.

Disturbed by Congress' recent decision proposing a 25% budget reduction for CISA, Amit penned a letter. It was co-signed by several esteemed CISOs, entrepreneurs and business leaders, including Nikesh Arora, Chair and CEO, Palo Alto Networks; George Kurtz, Co-Founder and CEO, CrowdStrike; and Ron Green, CSO, Mastercard.

What Congress apparently fails to understand is that if we cut funding, CISA would no longer have the resources necessary to monitor federal networks and provide the frontline national security defense they do today. When that happens, our adversaries will make sure that our infrastructure, now at critical risk, upon which they all depend for their stints in Congress, will become useless to us all.

Amit previously served as RSA's president, spearheading its transformation into one of the most successful global security companies, following its acquisition of NetWitness – the network forensics company he founded and led as CEO.

In this episode of Cybersecurity Insights, Amit discusses:

- The proposed reduction in CISA funding;
- The letter he authored, addressed to the U.S. Congress and co-signed by the industry's most influential practitioners;
- The increasing and ever-evolving global threat landscape;
- And much more.

Learn more by listening to the podcast here.

CYBERSECURITY INSIGHTS PODCAST

Get Smarter About AI and Large Language Models

Dan Grosu is a seasoned leader in the cybersecurity and IT sector, with over 20 years of experience in shaping technology strategies for startups and small to medium-sized businesses. Serving as CTO and CISO at Information Security Media Group Corp. (ISMG) for the last 14 years, Dan has been pivotal in building and managing the company's infrastructure from its inception, guiding its successful transition to cloud computing. His commitment to innovation and security is evident in his leadership, as he established a development team in Eastern Europe and pioneered various internal systems before the advent of mainstream tools. Prior to ISMG, Dan held key roles in organizations across banking, healthcare and automotive sectors, where he leveraged his technical expertise to drive significant security initiatives.

Looking ahead, Dan is committed to exploring artificial intelligence (AI) in cybersecurity, aiming to enhance industry practices and stay ahead of emerging trends. His combination of technical skills, leadership and forward-thinking makes Dan a widely respected leader in the cybersecurity community.

In this episode of Cybersecurity Insights, Dan and Steve discuss:

- Their perspective on technology and AI;
- The evolution of large language models (LLM);
- The role and importance of data;
- And much more.

Learn more by listening to the podcast here.

CYBERSECURITY INSIGHTS PODCAST

Understand Rising Cyber Governance Requirements

Jenny W. Hedderman Esq. is Risk Counsel in the Statewide Risk Management Team in the Massachusetts Office of the Comptroller. Attorney Hedderman specializes in compliance, internal controls, and risk management in the areas of statewide accounting, payroll, financial reporting, and statewide financial audits for 154 state agencies. Her current focus is developing the Comptroller's Statewide Risk Management program, including cybersecurity internal controls and cybersecurity awareness to reduce fraud and cyber incidents. Recent projects include the CTR Cyber Center website providing cybersecurity content, Cybersecurity Tips of the Week, CTR Cyber 5 and other internal controls to improve financial responsibility and protection of data, assets and resources across the Commonwealth. Attorney Hedderman is Chair of the State Records Conservation Board, Secretary of the Essex Co-Operative Farming Association Board, as well as Adjunct Professor in Business Law at Endicott College.

In this episode of Cybersecurity Insights, Jenny discuss:

- The Joe Sullivan case;
- Regulations concerning generative AI;
- Best practices in cyber governance;
- And much more.

Learn more by listening to the podcast here.

CYBERSECURITY INSIGHTS PODCAST

Navigating Conflicts and Corporate Controls

With more than two decades of experience in security, networking, computer science and control systems, Yossi Appleboum possesses a broad perspective on cybersecurity threats and innovative security solutions. Appleboum joined the Israeli Army Intelligence Corps (Unit 8200) in the early 1990s and served as a team leader and as Chief Architect focusing on the design and development of critical infrastructure network monitoring and security systems. In 1998, he co-founded WebSilicon, an Israeli company specializing in the development of advanced networking and security systems. As the Vice President leading the research and development team, he was involved in the design and implementation of more than 250 different systems for government agencies, integrators and vendors worldwide.

In this episode of Cybersecurity Insights, Yossi discuss:

- The prevailing situation in Israel;
- The state of corporate performance;
- Their strategy in navigating the conflict;
- And much more.

Learn more by listening to the podcast here.

Digital Forensics

- Computer Forensics Fundamentals
- Network Forensics Concepts
- Windos OS Forensics
- Mobile Device Forensics
- Reverse Engineering

Security Engineer

- Security Engineering
- Identity and Access Management
- Advanced Intrusion Detection
- Database Security
- Windows Server Security
- Threat Modeling
- DevSecOps
- Advanced Adversary Tactics Cyber Range

Learning Path Spotlights

CyberEd.io is a new category of online cybersecurity education, providing fundamental technical skills needed to train Cyber-Warriors in the art of detection, defense, and protection. We also strive to instill understanding about why reasoning matters, why adaptability matters, why thinking like hackers matters. We help students build a culture of cybersecurity and an appetite for continuous learning.

When we partner with an organization, we partner for life. Our mission is to help defeat adversaries on all fronts. Our podcasts dive into technologies and processes that are working against adversaries. Students have access to white papers and eBooks written by industry experts, and case studies that bring cybersecurity training to life. Our daily blog also keeps us all focused on key objectives and outcomes. And our Master Class series is taught by widely recognized cybersecurity thought leaders.

There are also hundreds of summit sessions available to help students understand cybersecurity requirements in Singapore, Italy, India, Hong Kong, and elsewhere around the world.

Our industry needs experts and analysts to examine and execute cybersecurity solution frameworks, DevSecOps experts to reinforce continuous integration and continuous delivery (CI/CD) pipeline security, and more/better trained security engineers, researchers, and leaders than our enemies rely on. We build strong teams, drive better results, generate greater unity and engineer a cybersecurity culture in each of the organizations with which we partner. In this issue, we highlight two Cyber-Warrior Learning Paths:

- Security Engineering
- Digital Forensics

Security Engineering

The significance of security engineering cannot be overstated. This course aims to equip you with the essential knowledge and skills required in a field integral to protecting information systems from cyber threats and vulnerabilities. With cyberattacks becoming more sophisticated, understanding the principles of designing, building, and maintaining secure systems is crucial for safeguarding sensitive data and ensuring the integrity of digital infrastructures.

Digital Forensics

The field of digital forensics is increasingly critical. This course is designed to introduce you to the science of uncovering and analyzing digital evidence collected from electronic devices. With growing incidents of cybercrimes and the need for data recovery in various legal and business contexts, the skills learned in this course are more relevant than ever.

+1-609-356-1499 • info@cybered.io • www.cybered.io

CyberEd MAGAZINE